REMARKS

Claims 1-59 are pending. Claims 1, 28, 49, 50 and 53 stand objected to. Claims 1-59 stand rejected under 35 U.S.C. § 112, ¶ 2 as being indefinite for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention. Claims 1-4, 6-7, 9-10, 12-13, 15-17, 19-21, 24-25, 28-29, 32-33, 36, 41.43 and 48 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,229,764 to Matchett. Claims 5, 8, 11, 14, 22-23, 26-27, 30-31, 34, and 44-47 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,229,764 to Matchett in view of U.S. Patent No. 5,655,116 to Kirk. Claims 18 and 37-40 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,229,764 to Matchett in view of European Patent No. 598469 to Dunlevy.

Reconsideration is requested. No new matter is added. The rejections are traversed. Claims 1-12, 17-19, 25-34, 36, 47-49, 52-54, and 59 are amended. Claims 1-59 remain in the case for consideration.

TELEPHONE INTERVIEW

On October 14, 2005, the undersigned held a telephone interview with Examiner Pich. The topics of conversation included the defective declaration, the claim objections, and the claim rejections under 35 U.S.C. § 112, ¶ 2 and § 102(b). The Examiner indicated that the problem with the declaration was that the application serial number was not provided in the checked field of the form. The undersigned offered to correct this defect and resubmit the declaration.

Regarding the claim objections, the undersigned argued that claim 50 was acceptable. The undersigned argued that while claim 49 described the system as using the Internet as a communication medium, this did not mean that every element in the system communicated using the Internet. Accordingly, claim 50 properly narrowed parent claim 49 by indicating a particular element did not use the Internet as a communication medium.

Regarding the claim rejections under 35 U.S.C. § 112, ¶ 2, the Examiner indicated that he preferred consistency among terms like "the" and "said" when referring to previously-mentioned claim elements, and that all adjectives associated with a particular element be included in such later uses. The undersigned indicated a willingness to clarify the claims consistent with the Examiner's preference.

Regarding the claim rejections under 35 U.S.C. § 102(b), the Examiner indicated a general agreement with the Applicant's argument that Matchett teaches an authentication

system, whereas the claimed invention is directed toward an identification system. The Examiner noted, however, that certain references use terms such as "identification" and "authentication" in inconsistent manners, and opined that a person skilled in the art might not automatically associate a particular process with the use of a particular term. The undersigned did not disagree that some references did not use the best term. Nevertheless, the undersigned argued that the terms still have meaning and would be properly understood. In addition, the undersigned pointed out that the claims themselves are more specific than just using the potentially uncertain terms, and that the claimed system, apparatus, or method was distinguishable from that described by Matchett based on the recited structure and operation. For example, claim 1 describes "the host system data processing center comparing the real time data with selected records". Note the use of the plural term "records", which indicates a one-to-many comparison. Matchett, regardless of terminology, teaches a one-to-one comparison, and thus is distinguishable. The Examiner acknowledged the Applicant's argument, but indicated a desire to consult with another Examiner before agreeing completely.

CLAIM OBJECTIONS

The Examiner objected to claims 1, 28, and 53 as using the term "and" where the term "or" should have been used. While the Applicant believes that "and" was clear, the term has been changed to "or" as requested by the Examiner.

The Examiner objected to claim 49 as including an unnecessary word "respecting". The Applicant apologizes for the error. A better word would be "representing". Data can represent things; this was what was intended in claim 49.

The Examiner objected to claim 50 as not narrowing the scope of the parent claim 49. The Examiner indicated that claim 49 described connections as using the Internet, and so claim 50, describing the data processing center connections as not being via the Internet, are not further limiting the claims. As discussed in the telephone interview of October 14, 2005, the Applicant believes that claim 49 does not require all connections to be via the Internet, and therefore claim 50 is properly narrowing the scope of parent claim 49.

REJECTIONS UNDER 35 U.S.C. § 112, ¶ 2

The Applicant has amended the claims to address the Examiner's rejections under 35 U.S.C. § 112, ¶ 2.

REJECTIONS UNDER 35 U.S.C. § 102(b)

Matchett generally

Matchett discloses an invention directed to preventing access to certain systems and devices, by using a biometrically-based authentication system that intermittently identifies a user, to improve system security (column 3, lines 10-14). Matchett indicates that biometric gate systems are not fool proof, since after an initial check, no other continued check is necessary to continue to use the system. Therefore, the motivation to provide intermittent biometric checks was to increase biometric check duration or number to enhance security (column 2, lines 47-52). Because of the increased number of biometric checks, Matchett predicts user unfriendliness. In order to solve that problem, Matchett suggests integrating his invention into the user interface, thereby making the user subject to passive biometric checks (column 3, lines 3-7). Matchett discloses repeated one-to-one biometric checks (column 3, lines 33-34; column 4, lines 61-64; column 6, lines 3-7; and column 6, lines 52-55). These one-to-one comparisons apply to all of the disclosed embodiments (column 4, lines 55-57).

There are several telling points about Matchett. The most important of these is that Matchett teaches an authentication system, not an identification system. An authentication system answers the question of "Am I who I say I am?" This is a very different question from "Who am I?", which is the question posed to a system performing identification. To perform authentication, the system simply compares the bid biometric against the registered biometric *for the person the user claims to be*. Either a match is found, or it is not. Thus, the system answers either "yes" or "no" to the question posed by the user ("Am I who I say I am?"). In contrast, an identification system does not have a starting point for the comparisons: it has to compare the bid biometric against all registered biometrics. And the answer is not a simple "yes" or "no": the system responds with "Mary," or "Joe," or "Fred," or (if no match was found) "no match found." The differences in question and answer between authentication and identification make the processes and supporting apparatuses very different.

The fact that Matchett teaches one-to-one comparisons with a pre-selected reference biometric sample is evidence that Matchett teaches an authentication system. The language of Matchett (down to the title of the invention) describes only an authentication system. For example, the process is described as "The microprocessor 114 then gathers the stored reference data from storage 112, and *sends both the reference data and the new data as indicated by signal line (H) to the comparison element*" (column 6, lines 3-6; emphasis

added). Therefore, the comparison step occurs after the reference data is chosen. This indicates that the process in Matchett is a one-to-one comparison.

In Matchett there is repeated comparison of a single bid biometric sample obtained from a user against a single biometric sample, to make a verification: not to make an identification. Matchett does not disclose a one-to-multiple comparison of a bid biometric sample against a library of more than one stored biometric samples. Nor can it be implied that Matchett's invention discloses matching a single bid biometric sample against a library of biometric samples, or even a subset of biometric samples. Matchett's inventions simply cannot be functional for large-scale user applications such as financial transactions used by millions of individuals. Although Matchett discloses numerous uses for his invention such as computer based gambling, access to individual or single cellular phones, military weapons systems, nuclear power plant controls, and space craft, financial transactions are not mentioned (column l, lines 34-43), one cannot impute to Matchett the possibility of tokenless access by millions of users of military weapons systems, nuclear power plants or gating the use of a single cellular phone with a centralized biometric data library.

A second telling fact about Matchett is that nowhere does Matchett, expressly or impliedly, teach that the user is aware that the system is being used. Indeed, the system of Matchett is designed to operate silently, so that users are not made unfriendly. In addition, were the user alerted to the fact that the system is re-testing the user's authorization, then users could deceive the system. The user with proper access would simply take over whenever the system began to re-test the user's authorization, then would relinquish control to a fraudulent user once re-testing was complete. Thus, giving the user notice of the system's operation would defeat the security measures the Matchett is designed to add.

Finally, Applicant submits that Matchett's device is a token-based invention. The comparison of a bid biometric to a single stored biometric, by definition, requires the use of a token. That is, once a system already knows to which specific stored biometrics a bid biometrics has to be compared to, the system must have used a token. Thus, while a token may take the form of a credit card or smart card, it can also be in the form of a specific device such as a single cellular phone or any operational device, which also contains the stored biometrics. As indicated above, Matchett only compares a bid biometric with only one stored biometric. Therefore, the process in Matchett, just like a credit card, is a process of verification, and not identification.

The claims are patentable over Matchett

Claim 1 is directed toward a system for providing voluntary tokenless biometric authorization, the system using at least one interconnecting means, the system comprising: at least one interconnecting means comprising any of the following: wide area network; X.25; ATM network; Internet network; cable television network; wireless network; and cellular telephone network; at least one gathering means for gathering real time data of biometric samples of an individual who is using the at least one gathering means, the at least one gathering means linked to the at least one interconnecting means; at least one computer network linked to at least one interconnecting means, access of the at least one computer network via the at least one interconnecting means being sought by the individual using the at least one gathering means and being dependent on the voluntary tokenless biometric authorization of the individual; and, at least one host system data processing center linked to at least one of the at least one gathering means and at least one of the at least one computer network so as to receive the real time data, the at least one host system data processing center having records of biometric data of one or more enrolled individuals, the at least one host system data processing center comparing the real time data with selected records, the comparison being to determine whether the real time data sufficiently matches the selected records as to authorize an individual seeking access to the at least one computer network, wherein the at least one host system data processing center communicates using one of the following: the at least one interconnecting means linked to the at least one gathering means, or the at least one interconnecting means linked to the at least one computer network; wherein the at least one host system data processing center conducts the voluntary tokenless biometric authorization without the individual being required to use a magnetic stripe card or a smart card.

Claim 28 is directed toward a method for providing voluntary tokenless biometric authorization, the method using at least one interconnecting means, the method comprising: a gathering step for gathering real time data of biometric samples, wherein the gathering step uses a gathering means; a biometric data transmittal step, wherein the real time data is transmitted to at least one host system data processing center, a comparison step, wherein the at least one host system data processing center, having records of biometric data of one or more enrolled individuals, compares the real time data with selected records, the comparison being to determine whether the real time data sufficiently matches the selected records as to authorize an individual seeking access to at least one computer network; a computer network access step, wherein upon successful voluntary tokenless biometric authorization of the

individual seeking access, the individual seeking access is enabled to access at least one computer network; an interconnecting means data transmittal step, wherein: the at least one interconnecting means comprises at least one of the following: wide area network; X.25; ATM network; Internet network; cable television network; wireless network; and cellular telephone network; for transmittal of data, the at least one host system data processing center communicates using at least one of the following: the at least one interconnecting means linked to at least one gathering means, or the at least one interconnecting means linked to at least one computer network; wherein the voluntary tokenless biometric authorization method is conducted without the individual seeking access being required to use a magnetic stripe card or a smart card.

Claim 49 is directed toward a system for providing biometric authentication, the system using the Internet as a communication medium, the system comprising: at least one gathering means station linked to the Internet, the at least one gathering means station providing selected real time data representing biometric characteristics of an individual who is using the gathering means station; at least one computer network linked to the Internet, access of the at least one computer network via the Internet being sought by the individual using the gathering means station and being dependent on authentication of the individual; and a data processing center linked to at least one of the gathering means and the at least one computer network so as to receive the real time data, the data processing center having records of biometric data of one or more enrolled individuals, wherein the data processing center compares the real time data with selected records, the comparison being to determine whether the real time data sufficiently matches the selected records as to authenticate an individual seeking access to the at least one computer network, and wherein, upon successful authentication of the individual, the data processing network transmits the voluntary tokenless biometric authorization to the at least one computer network.

Claim 54 is directed toward a method for Internet-based, biometric authentication of individuals who are using a gathering means station, the individuals seeking access of a computer network, the method comprising the steps of: establishing biometric characteristics to be used in authentication; acquiring, at the gathering means station, biometric data in accordance with the biometric characteristics; receiving, at a data processing center, a message that includes real time data; selecting, at the data processing center, one or more records from among records associated with one or more enrolled individuals; comparing, at the data processing center, real time data with selected records, the comparison determining whether the real time data sufficiently matches the selected records as to authenticate an

individual seeking access to the computer network; and, in the event of successful biometric authorization, transmitting from the data processing center, the biometric authorization to the computer network.

As discussed in the telephone interview held on October 14, 2005, the Examiner agreed to the difference between identification and authentication. As argued above, Matchett teaches a one-to-one comparison, which is authentication. In contrast, identification is a one-to-many comparison. This point is made in all of the independent claims. Specifically, claim 1 describes "the at least one host system data processing center comparing the real time data with selected records"; claim 28 describes "the at least one host system data processing center . . . compares the real time data with selected records"; claim 49 describes "the data processing center compares the real time data with selected records"; and claim 54 describes "comparing, at the data processing center, the real time data with selected records". In other words, all the independent claims describe comparing the data with a plurality of records, which means that the claimed invention is performing one-to-many comparison: in other words, identification.

Matchett's invention would be simply inoperative were it to be used to search the biometrics of over 100 million users, without a one-to-one comparison where the user identifies himself first. This is due to two reasons. First, Matchett requires that intermittent and multiple verifications be performed while the device is in use. Second, some of Matchett's embodiments further require the comparison of several types of biometrics, such as a fingerprint and voiceprint taken together, to make a single verification. The comparison of a single bid biometric with a library of millions of stored biometrics is a prohibitively time consuming process and commercially infeasible to implement in a system such as Matchett teaches. Therefore, requiring multiple comparisons or comparison of different types of biometrics would be inoperative if it did not require the use of tokens.

In addition, as argued above, Matchett teaches a system where the user is not aware that the system is being used. Finally, Matchett teaches a token-based system. The claimed invention operates with the user aware of its operation, and is tokenless: this term appears at the very beginning of the claims.

For these reasons, claims 1, 28, 49, and 54 are patentable under 35 U.S.C. § 102(b) over Matchett. Accordingly, claims 1, 28, 49, and 54, and dependent claims 2-27, 29-48, 50-53, and 55-59, are therefore allowable.

For the foregoing reasons, reconsideration and allowance of claims 1-59 of the application as amended is solicited. The Examiner is encouraged to telephone the undersigned at (503) 222-3613 if it appears that an interview would be helpful in advancing the case.

Respectfully submitted,

MARGER JOHNSON & McCOLLOM, P.C.

Ariel S. Rogson
Reg. No. 43,054

MARGER JOHNSON & McCOLLOM, P.C.
210 SW Morrison Street, Suite 400
Portland, OR 97204
503-222-3613
Customer No. 20575